



Sverm-problemstilling: AI-implementering i kommunalt foretak under juridisk og sikkerhetsmessig usikkerhet

Situasjonsbeskrivelse

Magnus er Chief Digital Officer i et kommunalt foretak med 200 ansatte som leverer digitale innbyggertjenester. Han står overfor pressing fra politikere om å implementere AI-løsninger for å modernisere tjenestene og forbli konkurransedyktig. Samtidig mottar han motstridende veiledning fra interne interessenter:

- **Juridisk avdeling:** Gir konservative tolkinger av GDPR-kravene og advarer mot å starte uten fullstendig juridisk avklaringer
- **IT-sikkerhet:** Oppgir sikkerhetskrav basert på NSM-veiledningen, men disse tolkes ulikt av juridisk avdeling
- **Leverandører:** Markedsfører løsninger som "GDPR-compliant" og "sikkerhetsklar", men gir ikke skriftlige garantier
- **Politikere:** Forventer rask handling og peker på at andre kommuner allerede implementerer AI

Sentrale spenningspunkter:

- Begge interne avdelinger dokumenterer sitt syn slik at Magnus blir eneperson som må bære ansvaret hvis noe går galt
- Juridisk grunnlag er objektivt uavklart (ikke bare for Magnus, men generelt i sektoren)
- Det er reell usikkerhet om GDPR tillater det bestemte AI-bruksområdet under de aktuelle prosesseringsbetingelsene
- Venting på full juridisk avklaring kan ta måneder eller år – og klaringen kan aldri komme hvis lovgivingen ikke blir presisert
- Konkurransetrykk fra andre kommuner som tar "akseptert risiko"-tilnærmingen nå

Konkret dilemma

Skal Magnus:

1. **Starte pilot nå** med eksplisitt akseptert juridisk grunnlag-usikkerhet (og risikoavklaring med politisk ledelse), eller



2. **Vente på klarhet** som kan ta ubestemmelig tid, med risiko for å bli oppfattet som passiv, eller
3. **Finne en tredje vei** – og hvis ja, hva konkret?

Spørsmål svermen skal besvare

1. **Risikostyring i grånyanser:** Hvordan kan Magnus kategorisere og dokumentere ulike grader av juridisk/sikkerhetsmessig usikkerhet, slik at han kan forsvare en pilot-tilnærming uten å fremstå som hensynsløs? Hva må til for at en “akseptert risiko” blir forsvarlighet i offentlig sektor?
2. **Ansvarsfordeling og dokumentasjon:** Hvordan kan Magnus få juridisk avdeling og IT-sikkerhet til å ta eksplisitt medansvar gjennom skriftlig risikovurdering, i stedet for å bare advare ham? Hvilken prosess sikrer at beslutningstaking blir kollektiv og sporbar?
3. **Leverandørkontraktbestemmelser:** Hvilke konkrete kontraktuelle tilbakekrav kan Magnus kreve for å senke risikoen når leverandøren ikke kan gi full compliance-garanti? (f.eks. skjold-klausuler, revisjonsrettigheter, ansvarsbegrensninger)
4. **Minimalstandarder for pilot:** Hva er det absolutte minimumsnivå av juridisk og teknisk tilrettelegging som gjør en pilot forsvarlig – uten å stille krav til perfektjonisme som gjør den umulig?
5. **Politisk strategisamtale:** Hvordan bør Magnus formulere valget overfor politisk ledelse slik at de tar et reelt, informert valg – i stedet for å delegere kompleksiteten ned til ham?
6. **Tidskompromiss:** Finnes det en midtveistrategi – f.eks. et begrenset pilot med spesifikke sikringsmekanismer – som gir politikerne noe å vise nå, samtidig som den gir rom for juridisk avklaring underveis?

Hva jeg IKKE trenger

- Generisk GDPR-intro eller “AI er både mulighet og risiko”
- Standardfraser som “økt transparens løser det” uten konkrete mekanismer
- Antagelser om at juridisk avdeling eller IT alltid har rett – eller at leverandøren lyver
- Råd om å “gå forbi” juridisk eller sikkerhet for å bevege seg raskere
- Teori om hva andre sektorer gjør; jeg trenger kommunal praksis eller dokumenterte kommunale presedens



- Rettslig analyse av GDPR (jeg har advokat for det); jeg trenger strategisk prosessdesign
-

Hva jeg TRENGER

- **Konkrete prosessmodeller** for hvordan risikoen kan løftes fra individ til organisasjon og politikk
- **Dokumentmaler eller sjekklister** som gjør “akseptert risiko” begripelig og juridisk robust
- **Pilotdesign-opsjoner** som balanserer handling/læring med forsvarlighet (ikke alt-eller-ingenting)
- **Eksempler fra kommune/offentlig sektor** der slike valg er gjort – og hva som skjedde
- **Innspill til hvordan Magnus skal språksette overfor sine avdelinger** – hvilke samtaler og møter er kritiske?
- **Tidsplan-alternativer** – eksplisitt: hvis han venter, hva bør skje i mellomtiden for å forberede?